

UNITED STATES DISTRICT  
COURT DISTRICT OF MINNESOTA  
Criminal No. 15-CR-11 (PJS/SER)

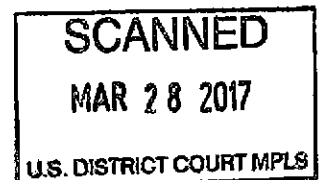
UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	<b>PLEA AGREEMENT AND</b>
	)	<b>SENTENCING STIPULATIONS</b>
v.	)	
	)	
MAXIM SENAKH,	)	
	)	
Defendant.	)	

The United States of America and Maxim Senakh (hereinafter referred to as the "Defendant") agree to resolve this case on the terms and conditions that follow. This plea agreement binds only Defendant and the United States Attorney's Office for the District of Minnesota. This agreement does not bind any other United States Attorney's Office or any other federal or state agency.

1. **Charges.** Defendant agrees to plead guilty to Count 1 of the Indictment, which charges Defendant with Conspiracy to Violate the Computer Fraud and Abuse Act and to Commit Wire Fraud, in violation of Title 18, United States Code, Section 371. The United States agrees to dismiss Counts 2 through 11 at the time of sentencing. The United States further agrees not to bring additional charges related to the offense conduct.

2. **Factual Basis.** The United States and Defendant agree on the following factual basis for the plea:

a. Beginning at least as early as 2008, Defendant voluntarily and intentionally entered into a conspiracy with an individual using the alias "Silver Fox," and



other, unidentified co-conspirators. The purpose of this conspiracy was to install malicious computer software ("malware") on thousands of computer servers located in Minnesota and throughout the world, to use that malware to generate internet traffic, and to monetize the traffic by directing it toward certain websites. The malware that was installed was known as "Ebury."

b. The defendant's co-conspirators deployed the Ebury malware on computer servers that ran using the Linux operating system.

c. The Ebury malware is capable of conducting several different illicit operations. Once it has infected a server, the Ebury malware harvested the log-on credentials used to access the infected server as well as the credentials for other servers that subsequently were accessed through the infected server. Then the Ebury malware exfiltrated the stolen credentials to another infected computer server under the control of members of the conspiracy. This provided members of the conspiracy with unauthorized "backdoor" access to and control over the infected computer servers.

d. Once the Ebury malware was installed on a computer server, the computer server could be controlled remotely by members of the conspiracy. For the purposes of this plea agreement, a computer server infected with malware that allows it to be controlled remotely, without the owner's knowledge or authorization, is referred to as a "bot." Collectively, a network of infected computer servers that collectively can be controlled remotely is referred to as a "botnet." The botnet infected with the Ebury malware was referred to as the Ebury Botnet. Members of the conspiracy used their unauthorized

access to install other malware and run programs on the bots without the owners' knowledge or authorization.

e. Members of the conspiracy used the Ebury Botnet to generate revenue by engaging in click-fraud and through mass Spam e-mailing.

f. The Defendant actively participated in, and generated revenue from, the click-fraud scheme. The click-fraud was accomplished by Defendant and his co-conspirators through the installation of additional malware on Ebury-infected computer servers. When users visited websites hosted on Ebury-infected computer servers, this particular malware automatically re-directed them from the website the user intended to visit, through the Ebury Botnet, to a separate website. That website was for an advertiser that had hired Defendant or other members of the conspiracy as an affiliate to direct traffic, ostensibly through legitimate means, to the advertiser's website. The redirection was programmed so that it would appear that the redirected web traffic came from a user who had "clicked" on an advertisement placed by Defendant or members of the conspiracy for that advertiser, when in fact, nobody had clicked on a legitimate advertisement and users were instead redirected unwittingly from another website.

g. Members of the conspiracy also used the Ebury Botnet, with defendant's knowledge, to send spam e-mail messages that number in the tens of millions, if not far more. "Spam" e-mail messages are unsolicited bulk commercial e-mail messages. The content of these spam e-mail messages was designed to entice users to click on links contained in the messages. When spam recipients clicked on the link, they would be routed

by an Ebury-infected computer server to the websites of advertisers for which the defendant's co-conspirators were an affiliate.

h. Both the click fraud redirection and spam components of the Ebury Botnet required the creation and maintenance of sophisticated infrastructure to take control and funnel the traffic created by the Ebury Botnet toward advertisers' websites. A critical part of this infrastructure was domains registered by members of the conspiracy. The names of these domains were created using a Domain Generation Algorithm ("DGA") that resulted in alphanumeric domain names of varying length. Once registered, these domain names were hosted on Ebury-infected servers that were used to exfiltrate stolen credentials from infected Ebury servers.

i. Defendant and his co-conspirators used e-mail accounts including pmadison12@gmail.com, vtakko@googlemail.com, and rasputgnig@googlemail.com, to create accounts with domain registrars: Public Domain Registry ("PDR"), DirectNIC, and Namecheap.

j. Defendant created the email account vtakko@googlemail.com in January 2009. In September 2011, Defendant used this e-mail account to create an account with PDR through Reseller Club. At some point after he created the vtakko@googlemail.com account and associated PDR account, Defendant transferred control over them to his co-conspirators. Members of the conspiracy, using this PDR account, registered various DGA-generated domain names that were utilized by the Ebury Botnet, including:

- i. alt9y1xendd.info
- ii. c0dbq5vc9o3e.info
- iii. c1b1fi2pdi8w1f.net
- iv. mag8ultejudt.biz
- v. map9ultejudt.net
- vi. oaxey7m0lde8s1v.info

Defendant knew that the domain names that members of the conspiracy were registering were going to be used as a part of the Ebury Botnet and that he was going to, and did, benefit financially.

k. Defendant knew that other co-conspirators, including "Silver Fox," were also registering other domain names that would be used to help set up the infrastructure necessary for the Ebury Botnet.

l. Defendant monetized the Ebury Botnet by knowingly exploiting traffic he knew had been redirected from websites that were hosted on Ebury-infected servers and directing it to adult websites for which Defendant was an advertising affiliate.

m. On or before February 18, 2011, using the alias "Mikhail Katsap" and the e-mail address "katsepsacc@gmail.com," Defendant became an advertising affiliate for Adult Friend Finder ("AFF") with the intent of using this position to fraudulently obtain payments from AFF. AFF assigned Defendant the GPID "g242405" and the PID "p1011105." These identifiers were included in the AFF web addresses such that AFF could keep track of Defendant's redirected traffic and pay him accordingly.

n. On or about February 27, 2014, using Ebury malware, Defendant and others caused one or more visitors to the Thai-language website “dek-zaa.com,” to be unwittingly and automatically re-directed through the Ebury Botnet to an AFF website, which included Defendant’s assigned GPID and PID. The traffic was redirected to AFF in a manner that did not allow AFF to know it was receiving redirected traffic. The redirection made it appear to AFF that the visitors had “clicked” on an AFF advertisement placed by the defendant when in reality they had been unwittingly redirected.

o. Similarly, on or about January 15, 2014, Defendant and members of the conspiracy caused one or more visitors to the websites “photographersupplystation.com” and “myphotohome.com,” to be unwittingly and automatically redirected through the Ebury Botnet to an AFF website, which included the Defendant’s assigned GPID and PID. The redirection was done using the defendant’s assigned GPID and PID so that it appeared to AFF that the visitors had “clicked” on an AFF advertisement placed by the defendant when in reality they had been unwittingly redirected.

p. Defendant knew that the traffic he was sending to AFF was the result of traffic that was being redirected through the Ebury Botnet and was not generated from legitimate advertisements. Defendant’s actions defrauded AFF as AFF paid him for the illegitimate traffic. AFF paid Defendant and the co-conspirators \$228,018.56.

q. Defendant knew that other co-conspirators, including “Silver Fox,” were monetizing the Ebury Botnet by using it to send thousands of spam messages that contained links designed to entice recipients to “click” on them. Once users clicked on

these links, they would be routed through the Ebury Botnet to websites for which "Silver Fox" was acting as an affiliate.

3. **Waiver of Pretrial Motions.** Defendant understands and agrees he has certain rights to file pretrial motions in this case. As part of this plea agreement, and based upon the concessions of the United States contained herein, Defendant knowingly, willingly, and voluntarily gives up the right to litigate those pretrial motions and/or to file additional pretrial motions in this case.

4. **Statutory Penalties.** The parties agree that Count 1 of the Indictment carries statutory penalties of:

- a. a maximum sentence of 5 years' imprisonment;
- b. a supervised release term of up to 3 years;
- c. a fine of up to \$250,000;
- d. a mandatory special assessment of \$100; and
- e. payment of mandatory restitution in an amount to be determined by the Court.

5. **Revocation of Supervised Release.** Defendant understands that, if he violates any condition of supervised release, he could be sentenced to an additional term of imprisonment up to the length of the original supervised release term, subject to the statutory maximums set forth in 18 U.S.C. § 3583.

6. **Guideline Calculations.** The parties acknowledge Defendant will be sentenced in accordance with 18 U.S.C. § 3551, *et seq.* Nothing in this plea agreement should be construed to limit the parties from presenting any and all relevant evidence to

the Court at sentencing. The parties also acknowledge the Court will consider the United States Sentencing Guidelines in determining the appropriate sentence and stipulate to the following guideline calculations:

- a. Base Offense Level. The parties agree that the base offense level is 6. (U.S.S.G. § 2B1.1(a)(2)).
- b. Specific Offense Characteristics. The parties agree that the base offense level should be increased by 16 levels because the loss exceeded \$1,500,000, but was less than \$3,500,000. (U.S.S.G. § 2B1.1(b)(1)(I)). The parties also agree that the base offense level should be increased by 2 levels because the offense involved more than 10 victims. (U.S.S.G. § 2B1.1(b)(2)(A)(i)). The parties agree that the base offense level should be increased by 2 levels because the offense involved sophisticated means and Defendant intentionally engaged in or caused the conduct constituting sophisticated means. (U.S.S.G. § 2B1.1(b)(10)(C)). The parties agree no other specific offense characteristics apply.
- c. Chapter 3 Adjustments. The government agrees to recommend that Defendant receive a 3-level reduction for acceptance of responsibility and to make any appropriate motions with the Court. However, Defendant understands and agrees that this recommendation is conditioned upon the following: (i) Defendant testifies truthfully during the change of plea and sentencing hearings, (ii) Defendant cooperates with the Probation Office in the pre-sentence investigation, and (iii) Defendant commits no further acts inconsistent with acceptance of responsibility. (U.S.S.G. § 3E1.1(a) and (b)). The parties agree that no other Chapter 3 adjustments apply.
- d. Criminal History Category. Based on information available at this time, the parties believe that Defendant's criminal history category is I. This does not constitute a stipulation, but a belief based on an assessment of the information currently known. Defendant's actual criminal history and related status will be determined by Court based on the information presented in the Presentence Report and by the parties at the time of sentencing. Defendant understands that if the presentence investigation reveals any prior adult or juvenile sentence which should be included within his criminal history under the U.S. Sentencing Guidelines, Defendant will be sentenced based on his true criminal history category, and he will not be permitted to withdraw from this Plea Agreement. (U.S.S.G. § 4A1.1).



- e. Guideline Range. If the adjusted offense level is 23 and the criminal history category is I, the Sentencing Guidelines range is 46-57 months of imprisonment.
- f. Fine Range. If the adjusted offense level is 23, the fine range is \$20,000 to \$200,000. (U.S.S.G. § 5E1.2(c)(3)).
- g. Supervised Release. The Sentencing Guidelines advise a term of supervised release of between one to three years. (U.S.S.G. §5D1.2(a)(2)).
- h. Sentencing Recommendations and Departures. The parties reserve the right to make a motion for departures from the applicable Guidelines range and to oppose any such motion made by the opposing party. The parties reserve the right to argue for a sentence outside the applicable Guidelines range.

7. **Discretion of the Court.** The foregoing stipulations are binding on the parties, but do not bind the Court. The parties understand that the Sentencing Guidelines are advisory and their application is a matter that falls solely within the Court's discretion. The Court may make its own determination regarding the applicable Guideline factors. If the Court determines that the applicable Guideline calculations are different from that stated above, the parties may not withdraw from this agreement, and Defendant will be sentenced pursuant to the Court's determinations.

8. **Special Assessment.** The Guidelines require payment of a special assessment in the amount of \$100.00 for each felony count of which Defendant is convicted. (U.S.S.G. § 5E1.3). Defendant agrees the special assessment in the amount of \$100 is due and payable at the time of sentencing.

9. **Restitution.** Defendant understands and agrees that the Mandatory Victim Restitution Act, 18 U.S.C. § 3663A, applies and that the Court is required to order

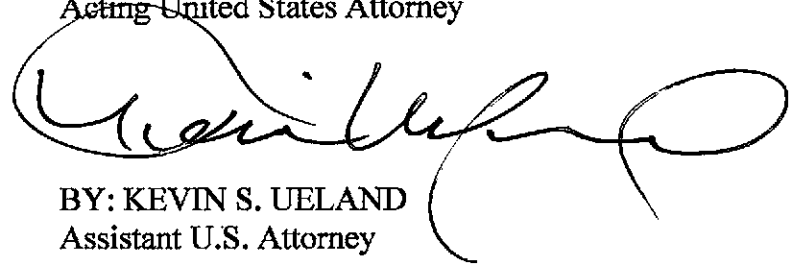
Defendant to make restitution to the victim(s) of his crime. There is no agreement on restitution at this time.

10. **Waiver of Trial.** Defendant understands that by pleading guilty he will waive all rights to a trial or appeal on the question of his guilt.

11. **Complete Agreement.** This is the entire agreement and understanding between the United States and Defendant.

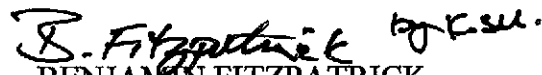
Date: 3/28/2017

GREGORY G. BROOKER  
Acting United States Attorney



BY: KEVIN S. UELAND  
Assistant U.S. Attorney


Date: 3/28/2017

  
BENJAMIN FITZPATRICK  
Senior Counsel  
U.S. Department of Justice  
Criminal Division  
CCIPS

Date: 3/28/2017

  
MAXIM SENAKH  
Defendant

Date: 3/28/17

  
MANVIR K. ATWAL  
Counsel for Defendant